Gordon-Mills-Welch差集合について (デザインの構成と解析)

AUTHOR(S):

山本, 幸一

CITATION:

山本, 幸一. Gordon-Mills-Welch差集合について (デザインの構成と解析). 数理解析研究所講究録 1977, 311: 86-97

ISSUE DATE:

1977-10

URL:

http://hdl.handle.net/2433/103895

数理解析研究所講究録
311巻 1977年 86-97

Gordon-Mills-Welch 差集合について

東女大 文理 山本幸一

1. Singer の差集合.

記号：q は素数 p の中 $q=p^h$, $F=GF(q)$, $K=GF(q^n)$, $n\geqq 2$. K の部分集合 A について $A^*=A-\{0\}$. 特に $F^*A^*\subset A^*$ ならば, A^*/F^* は巡回群 K^*/F^* の部分集合とみなす. K は F 上 n 次元ベクトル空間で, K の基本双一次形式

$$f(\xi,\eta)=S_{K/F}\,\xi\eta$$

がある. それは K/F が分離拡大であるためである. また

$$S_{K/F}\,\xi=\xi+\xi^q+\xi^{q^2}+\cdots+\xi^{q^{n-1}}$$

一次函数 $S_{K/F}$ の核を $D_{K/F}$ であらわす:

$$D_{K/F}=\{\xi;\ S_{K/F}\,\xi=0\}.$$

さらに超平面

$$E_{K/F}=\{\xi;\ S_{K/F}\,\xi=1\}$$

とおけば, 直和直積分解

$$K=D_{K/F}\dotplus F^*E_{K/F}$$

が成立つ. この際次の定理がある.

Singer の定理. $\bar{D}_{K/F} = D^*_{K/F}/F^*$ は巡回群 K^*/F^* 上の差集合である. そのパラメータは

$$v = \frac{q^n-1}{q-1}, \quad k = \frac{q^{n-1}-1}{q-1}, \quad \lambda = \frac{q^{n-2}-1}{q-1}.$$

上記の差集合 $\bar{D}_{K/F}$ を, 拡大 K/F に対応する Singer 差集合と言う.

[注意] K^* の生成元を α とすると, Singer 差集合は, 普通の巡回加法群の形では

$$\{m ; S_{K/F}(\alpha^m) = 0\} \qquad m \left(\mathrm{mod}\ \frac{q^n-1}{q-1}\right)$$

と書ける. すなわち Singer 集合は長さ q^n-1 のいわゆる M 系列 (maximal-length shift-register sequence) の零点の集合であるとも定義することができる.

2. Singer 集合の multiplier について.

定理 1. $n \geq 3$ ならば, Singer 集合 $\bar{D}_{K/F}$ の multiplier は p の巾だけである.

[証明] Singer 集合が '標準形' の差集合であることから r が一つの multiplier であるための条件は

$$D^r_{K/F} = D_{K/F},$$

すなわち

$$(1) \qquad S_{K/F}\,\xi = 0 \iff S_{K/F}\,\xi^r = 0$$

で与えられる.

これが成立てばKの写像

$$R:\ \xi \longrightarrow \xi^r$$

は超平面 $D_{K/F}$ をそれ自身の上に写す．しかしKの超平面はすべて $f(\alpha,\xi)=0$，$\alpha\in K^*$ の形である．すなわち $\alpha^{-1}D_{K/F}$ の形だから，写像Rでは $\alpha^{-r}D_{K/F}^{r}=\alpha^{-r}D_{K/F}$ に，つまり超平面にうつされる．さてKの任意の線型部分空間 $\mathfrak{M}$ は，いくつかの超平面の共通部分であって，写像Rによって，いくつかの超平面の共通部分にうつされる．すなわちRは $\mathfrak{M}$ をそれと同一次元の線型部分空間にうつす．そのような r が p の中以外にないというのが定理1の内容である．

われわれの仮定の下では，たとえば $\alpha_1,\alpha_2,\dots,\alpha_s$ が一次従属ならば $\alpha_1^r,\alpha_2^r,\dots,\alpha_s^r$ も一次従属で逆も真である．ゆえに $\xi\neq F$ に F^* の元 c_ξ を対応させて

(2) $\qquad 1=c_\xi\xi^r+c_\eta\eta^r \qquad$ (ただし $1=\xi+\eta$ とおく)

の成立するようにできる．むろん c_ξ は一意に定まる．この際まず乗法的の性質

(3) $\qquad c_{\xi\eta}=c_\xi c_\eta \qquad (\xi,\eta,\xi\eta\neq F)$

に注目する．上式はまず (2) より

$$\begin{aligned}1&=c_\xi\xi^r+c_{1-\xi}(1-\xi)^r\\&=c_\xi\xi^r\left(c_\eta\eta^r+c_{1-\eta}(1-\eta)^r\right)+c_{1-\xi}(1-\xi)^r\\&=c_\xi c_\eta(\xi\eta)^r+c_\xi c_{1-\eta}\left(\xi(1-\eta)\right)^r+c_{1-\xi}(1-\xi)^r\end{aligned}$$

だが，さらに

$$1 = c_{\xi\eta}(\xi\eta)^r + c_{1-\xi\eta}(1-\xi\eta)^r$$
$$= c_{\xi\eta}(\xi\eta)^r + c_{1-\xi\eta}\left(d_1(\xi(1-\eta))^r + d_2(1-\xi)^r\right)$$

だから，もし $1, \xi, \xi\eta$ が一次独立ならば $c_{\xi\eta} = c_\xi c_\eta$ となる．同様にして $1, \eta, \xi\eta$ が一次独立でも $c_{\xi\eta} = c_\xi c_\eta$ である．

ところでもし $1, \xi, \xi\eta$ が一次従属で，$1, \eta, \xi\eta$ が一次従属ならば，ξ 及び η は K の2次の部分体 $F(\xi\eta)$ に含まれる．しかし定理の仮定から $n \geqslant 3$ であるから，その2次体に含まれない元 ζ が存在する．そして $1, \xi\eta, \xi\eta\zeta$ は一次独立で，$c_{\xi\eta\zeta} = c_{\xi\eta} c_\zeta$．また同様に $c_{\xi\eta\zeta} = c_\xi c_{\eta\zeta} = c_\xi c_\eta c_\zeta$．これから $c_{\xi\eta} = c_\xi c_\eta$ が一般に成立つ．

次に $\omega \in F^*$ に対しても c_ω を定義するのには，$\xi, \eta, \xi\eta \notin F$ のとき (3) より $c_{\omega\xi\eta} = c_{\omega\xi} c_\eta = c_\xi c_{\omega\eta}$．すなわち $c_{\omega\xi} c_\xi^{-1}$ は ξ に依存しない．これをもって c_ω を定めればよい．そうすると $\xi \longrightarrow c_\xi$ は K^* から F^* の中への準同型であることが容易に分る．ゆえに $c_\xi = (N_{K/F}\xi)^t$，t 定数，となる．

さて (1) において r を $r + tv$，$v = (q^n - 1)/(q-1)$ で置き換えるならば (2) の函数 c_ξ は $c_\xi (N_{K/F}\xi)^{-t}$ で置きかわる．ゆえに r をそれと $(\mathrm{mod}\, v)$ で合同な数で置き換えて，始めから $c_\xi = 1$ であると仮定してもよい．この際 ξ と η が一次独立ならば，

$$(\xi+\eta)^r=\xi^r+\eta^r$$

が成立する．同式が一次従属なる ξ,η に対しても成立することは容易に証明される．よって $R:\xi\longrightarrow\xi^r$ は，体 K の自己同型となり，r は p の中と $(\mathrm{mod}\ q^n-1)$ で合同である．

3. Gordon-Mills-Welch の合成．

定理2. 体の塔 $F\subset L\subset K$，$F=GF(q)$, $L=GF(q^m)$, $K=GF(q^{mn})$, $m\geqslant 2$, $n\geqslant 2$ があったとき，L^*/F^* 上の差集合 $\bar{\Delta}$ はパラメータ

$$v=\frac{q^m-1}{q-1},\quad k=\frac{q^{m-1}-1}{q-1},\quad \lambda=\frac{q^{m-2}-1}{q-1}$$

をもつものとして，L^* の部分集合 Δ は

$$\Delta F^*\subset\Delta,\quad \Delta/F^*=\bar{\Delta}$$

なるものとする．このとき

$$D=D_{K/L}\dot{+}\Delta E_{K/L}$$

とおけば，$\bar{D}=D^*/F^*$ は K^*/F^* 上の差集合で，パラメータ

$$v=\frac{q^{mn}-1}{q-1},\quad k=\frac{q^{mn-1}-1}{q-1},\quad \lambda=\frac{q^{mn-2}-1}{q-1}$$

をもつ．

[証明] D は $S_{K/L}\xi\in\Delta\cup\{0\}$ を満たすもの集合である．さて $\theta\in\Delta$ のとき，"超平面" $\theta E_{K/L}=\{\xi;\ S_{K/L}\xi=\theta\}$ は丁度 $q^{m(n-1)}$ 個の元を含み，超平面 $D_{K/L}$ も同様であるから，

$\#(\Delta \cup \{0\}) = q^{m-1}$ より，D は J 度 q^{mn-1} 個の元から成る．

証明に必要なのは $\alpha \in K^*, \notin F^*$ のとき $\#(D \cap \alpha D) = q^{mn-2}$ となる事実である．

まず $\alpha \in L^*$ であれば $\xi \in D \cap \alpha D$ と同等な条件

$$\begin{cases} S_{K/L}\xi = \theta_1 \in \Delta \cup \{0\}, \\ S_{K/L}(\alpha^{-1}\xi) = \alpha^{-1} S_{K/L}\xi = \theta_2 \in \Delta \cup \{0\} \end{cases}$$

をみたす ξ の個数 $\#(D \cap \alpha D)$ は，等式

$$\theta_2 = \alpha\theta_1, \quad \theta_1 \in \Delta \cup \{0\}, \quad \theta_2 \in \Delta \cup \{0\}$$

の解の個数 λ_α によって $\#(D \cap \alpha D) = \lambda_\alpha q^{m(n-1)}$ で与えられる．しかし Δ が差集合だから，$\alpha \in L^*, \notin F^*$ なら $\lambda_\alpha = q^{m-2}$ で，これから $\#(D \cap \alpha D) = q^{mn-2}$ が得られる．

次に $\alpha \notin L^*$ ならば，$\xi \in D \cap \alpha D$ と同等な条件

$$\begin{cases} S_{K/L}\xi = \theta_1 \in \Delta \cup \{0\}, \\ S_{K/L}(\alpha^{-1}\xi) = \theta_2 \in \Delta \cup \{0\} \end{cases}$$

のおのおのは，平行でない超平面で，$q^{m(n-2)}$ 個の元を共有する．ここでは θ_1, θ_2 がそれぞれ $\Delta \cup \{0\}$ の中を自由に動くので，$\#(D \cap \alpha D) = q^{mn-2}$ となる．

定理2で与えられた差集合 $\bar{D}$ は，L^*/F^* の差集合 $\bar{\Delta}$ と Singer 集合 $\bar{D}_{K/L}$ の Gordon-Mills-Welch 式合成と呼び，これを

$$\bar{D} = \bar{D}_{K/L} \oplus \bar{\Delta}$$

で表わす.

定理3. 定理2の条件を満足する L^*/F^* 上の2つの差集合 $\bar{\Delta}_1$, $\bar{\Delta}_2$ がともに標準型で, しかも $\bar{D}_{K/L} \oplus \bar{\Delta}_1$ と $\bar{D}_{K/L} \oplus \bar{\Delta}_2$ とが同型であるならば, $\bar{\Delta}_1 = \bar{\Delta}_2$ である.

標準型であるという制限は本質的なものではないが, 証明を簡単にするために, 置いたものである.

証明に際しては著名な M. Hall の multiplier 定理を引用する. 現実的には《パラメータが

$$v = \frac{q^N-1}{q-1}, \quad k = \frac{q^{N-1}-1}{q-1}, \quad \lambda = \frac{q^{N-2}-1}{q-1}, \quad N \geqq 2$$

の差集合について p が一つの multiplier である》という特殊の場合であり, 我我が主として考察する差集合(後述)に対しては自動的に成立している事実である.

補題. 定理2の情況の下において

$$D \cap \xi L^* = \xi L^* \qquad (\xi \in D_{K/L}),$$

$$D \cap \xi L^* = \xi (S_{K/L}\xi)^{-1}\Delta \qquad (\xi \in D,\ \xi \notin D_{K/L}).$$

すなわち, $\xi \in D^*$ のとき, "算術級数" ξL^* は, $\xi \in D_{K/L}$ であるか否かに従い, q^m-1 個 あるいは $q^{m-1}-1$ 個の元を D と共有する. これによって D を分解する体 L を特長づけることができる.

[証明] 前出の K の直和直積分解

$$K = D_{K/L} \dotplus L^* E_{K/L}$$

に“適合する” D の分解が

$$D = D_{K/L} \dotplus \Delta E_{K/L}$$

であることを考慮すれば，まず $\xi \in D_{K/L}$ ならば $L^*\xi \subset D_{K/L}$，$L^*\xi \cap D_{K/L} = L^*\xi$．　また $\xi \notin D_{K/L}$ ならば上記分解から

$$\xi = \lambda\theta\ ,\ \lambda \in L^*\ ,\ \theta \in E_{K/L}$$

だから，$\lambda = S_{K/L}\xi$ ，$\theta = \xi(S_{K/L}\xi)^{-1}$ であって，

$$D \cap \xi L^* = D \cap \theta L^* = L^* E_{K/L} \cap L^*\theta \cap D = L^*\theta \cap \Delta E_{K/L} = \theta\Delta$$

となる．

[定理３の証明] 今“一次変換” $\xi \longrightarrow \beta\xi^\tau$ で $\bar{D}_1$ が $\bar{D}_2$ にうつるならば，$\bar{\Delta}_1, \bar{\Delta}_2$ が標準型であることから $\beta \in K^*$ が必要であるから，始めから $\beta = 1$ と取ってもよい．写像 $\xi \longrightarrow \xi^\tau$ によって D_1 が D_2 に移るものと仮定する．この時

$$D_1^\tau = D_{K/L}^\tau \dotplus \Delta_1^\tau E_{K/L}^\tau = D_2 = D_{K/L} \dotplus \Delta_2 E_{K/L}\ .$$

ここで前記の補題によって

$$D_{K/L}^\tau = D_{K/L}\ ,\quad \Delta_1^\tau E_{K/L}^\tau = \Delta_2 E_{K/L}$$

が得られる．

後者において $\xi \notin D_{K/L}$ ならば

$$(\xi L^* \cap D_1)^\tau = \xi^\tau L^* \cap D_1^\tau = \xi^\tau L^* \cap D_2\ .$$

補題によって書き替えると

$$(\xi(S_{K/L}\xi)^{-1})^\tau \Delta_1^\tau = \xi^\tau (S_{K/L}\xi^\tau)^{-1}\Delta_2\ .$$

ゆえに

$$z_\xi = \frac{S_{K/L}\,\xi^r}{(S_{K/L}\,\xi)^r} \in F^*$$

が必要である.

これから定理1の証明に移行して, それを繰返すのだが, (2) で定義された元 $c_\xi \in L^*$ は, 現在の場合 F^* に属することが次のようにして知られる.

すなわち $\xi \notin L$ の時, ξ と $1-\xi=\eta$ は L 上一次独立であるから

$$S_{K/L}(\xi\zeta)=1\,,\quad S_{K/L}(\eta\zeta)=0$$

を成立させる $\zeta \in K$ がある. (2) より

$$\zeta^r = c_\xi(\xi\zeta)^r + c_\eta(\eta\zeta)^r,$$

$$S_{K/L}\,\zeta^r = c_\xi\, S_{K/L}(\xi\zeta)^r + c_\eta\, S_{K/L}(\eta\zeta)^r.$$

すなわち, $z_\zeta = c_\xi z_{\xi\zeta} + 0$, $c_\xi = z_\zeta z_{\xi\zeta}^{-1} \in F^*$.

従って $\xi \longrightarrow c_\xi$ は K^* から (L^* の中にではなく), F^* の中への準同型に拡張されて, 前のように

$$c_\xi = (N_{K/F}\,\xi)^t$$

なる定数 t が存在する. そして r を $r + t(q^{mn}-1)/(q-1)$ で置きかえると, それは p の巾と $(\mathrm{mod}\ q^{mn}-1)$ で合同になる. しかしその際 Hall の multiplier 定理から $\Delta_1^r = \Delta_1$ で, $\Delta_2 = \Delta_1^r = \Delta_1$ でなければならない.

4. 体の塔に関するSinger集合の逐次合成.

体の塔 $F=K_0\subset K_1\subset K_2\subset\cdots\subset K_{s-1}\subset K_s=K$,

$$K_i=GF\left(q^{m_1m_2\cdots m_i}\right),\quad m_i\geqslant 2\qquad (i=1,\cdots,s),$$

$$K_0=GF(q),\quad K=GF(q^n)$$

の場合 $\bar{D}^{t_1}_{K_1/K_0}$, $\bar{D}^{t_2}_{K_2/K_1}$, $\cdots$, $\bar{D}^{t_s}_{K_s/K_{s-1}}$ を次次と合成して Gordon-Mills-Welch 型の差集合を得る. ここに $t_1, t_2, \cdots, t_s$ は

$$\left(t_i, \frac{q^{m_1m_2\cdots m_i}-1}{q-1}\right)=1$$

なる整数である. 具体的な形は, たとえば $s=4$ の場合

$$D_{K_4/K_3}\dot{+}E_{K_4/K_3}\left(D_{K_3/K_2}\dot{+}E_{K_3/K_2}\left(D_{K_2/K_1}\dot{+}E_{K_2/K_1}D^{t_1}_{K_1/K_0}\right)^{t_2}\right)^{t_3}$$

で, 略記法では

$$\bar{D}_{K_4/K_3}\oplus\left(\bar{D}_{K_3/K_2}\oplus\left(\bar{D}_{K_2/K_1}\oplus\bar{D}^{t_1}_{K_1/K_0}\right)^{t_2}\right)^{t_3}.$$

またそれは,

$$t_ir_i\equiv 1\pmod{\frac{q^{m_1m_2\cdots m_i}-1}{q-1}}$$

なる r_i を使って

$$S_{K_1/K_0}\left(S_{K_2/K_1}\left(S_{K_3/K_2}\left(S_{K_4/K_3}\xi\right)^{r_3}\right)^{r_2}\right)^{r_1}=0$$

なる ξ の集合を $\bmod F_0^*$ で取ったものとなる.

$m_1, m_2, \cdots, m_s$ を与えた時, $q=p^h$ ならば, 以上の形の差集合中で非同値なものの個数は

$$\prod_{i=1}^{s-1}\frac{1}{hm_1m_2\cdots m_i}\varphi\left(\frac{q^{m_1m_2\cdots m_i}-1}{q-1}\right)$$

で与えられる. ただし $m_1=2$ の場合には, 対応する因数

$\frac{1}{2h}\varphi(q+1)$ の所には，1 を代用するものとする．そして，それ以外では因数が $\geqq 2$ となる．このことは -1 が非自明 $(\lambda>0)$ なる差集合の multiplier ではないという一般論からの結論であるが，-1 が multiplier でないことをこの場で直接に示すならば，(2) から $\xi \neq F$ のとき

$$1 = c_\xi \xi^{-1} + c_{1-\xi}(1-\xi)^{-1}, \qquad c_\xi \in F^*,\ c_{1-\xi} \in F^*.$$

ξ は F 上 2 次方程式の根で，$n=2$ が必要となるからである．

定理 4. 他に同様の体の塔

$$F = K_0' \subset K_1' \subset \cdots \subset K_{s'-1}' \subset K_{s'}' = K,$$
$$K_i' = GF(q^{m_1' m_2' \cdots m_i'}),\quad m_i' \geqq 2 \quad (i=1,\cdots,s')$$

があって $(m_s, m_{s'}')=1$ であり，しかも

$$\left(\bar{D}_{K_s/K_{s-1}} \oplus \left(\bar{D}_{K_{s-1}/K_{s-2}} \oplus \left(\cdots \oplus \left(\bar{D}_{K_2/K_1} \oplus \bar{D}_{K_1/K_0}^{t_1}\right)^{t_2}\cdots\right)^{t_{s-1}}\right)^{t_s}\right.$$
$$= \bar{D}_{K_{s'}'/K_{s'-1}'} \oplus \left(\bar{D}_{K_{s'-1}'/K_{s'-2}'} \oplus \left(\cdots \oplus \left(\bar{D}_{K_2'/K_1'} \oplus \bar{D}_{K_1'/K_0'}^{t_1'}\right)^{t_2'}\cdots\right)^{t_{s'-1}'}\right.$$

ならば t_s は $\left(\mathrm{mod}\ \frac{q^n-1}{q-1}\right)$ で p の中と合同で，この差集合は

$$\bar{D}_{K/K_{s-1}\cap K_{s'-1}'} \oplus \left(\bar{D}_{K_{s-1}\cap K_{s'-1}'/L} \oplus \left(\cdots\cdots\right)\cdots\right)^t$$

の形に書くことができる．すなわち塔

$$F = L_0 \subset \cdots\cdots \subset L_{r-1} = K_{s-1}\cap K_{s'-1}' \subset L_r = K$$

に対する逐次合成と見なすことができる．これによって種種の体の塔に対する差集合の中の非同値なものの個数は前掲の

ものの和として表わすことができる。その具体的な形は省略する。また定理4の証明には多少の準備を必要とするので，ここでは省略することにする。

文献

B. Gordon, W. H. Mills and L. R. Welch: Some new difference sets, Canad. Journ. Math., vol. 14 (1962), 614-625.

M. Hall, Jr.: Combinatorial Theory, Blaisdell, 1967.

L. D. Baumert: Cyclic difference sets, Math. Lecture Notes, No. 182, 1972.

K. Yamamoto: On the Gordon-Mills-Welch difference sets, 近刊.